Tina Wolfson (SBN 174806)
Robert Ahdoot (SBN 172098)
Theodore W. Maya (SBN 223242)
Bradley K. King (SBN 274399)
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com
rahdoot@ahdootwolfson.com
tmaya@ahdootwolfson.com
bking@ahdootwolfson.com

Gary M. Klinger (*pro hac vice to be filed*)
MILBER COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ALLEN SHAKIB, individually and on behalf of all others similarly situated,

Plaintiff,

v.

COINBASE GLOBAL, INC. and COINBASE, INC.,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Allen Shakib, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendants Coinbase Global Inc., and Coinbase, Inc. (together, "Coinbase" or "Defendants").

NATURE OF THE ACTION

1. Plaintiff brings this class action individually and on behalf of all other individuals who had their sensitive personally identifiable information[1] including names, addresses, phone numbers, and email addresses, Social Security numbers (SSN), bank-account numbers and some bank account identifiers, Government-ID images (e.g., driver's license, passport, account data (balance snapshots and transaction history); and limited corporate data (including documents, training material, and communications available to support agents (collectively, "PII" or "Personal Information") disclosed to unauthorized third parties during a Data Breach compromising Coinbase in or around May 2025 (the "Data Breach").

2. Coinbase is the largest U.S. based cryptocurrency exchange, with over 100 million users and a trading volume of $468 billion.[2] Its stated purpose is to "increase economic freedom in the world" by "updat[ing] the century-old financial system by providing a trusted platform" to trade cryptocurrencies.[3]

3. On May 15, 2025, Coinbase publicly disclosed a Data Breach involving cybercriminals who recruited and bribed rogue overseas support agents to steal sensitive personal data from Coinbase's

[1] Personally identifiable information ("PII") includes information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

[2] *See* Coinbase Global, Inc., Form 10-K (Feb. 13, 2025), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001679788/000167978825000022/coin-20241231.htm.

[3] Investor Relations, COINBASE, https://investor.coinbase.com/home/default.aspx (last accessed May 15, 2025).

internal systems and then demanded a $20 million ransom not to publish the stolen information. Coinbase has not paid the demand and is cooperating with law enforcement in the investigation of the Data Breach.[4]

4. According to Coinbase, on May 11, 2025, it "received an email communication from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase documentation, including materials relating to customer-service and account-management systems."[5] The cybercriminals "obtained this information by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems to which they had access in order to perform their job responsibilities. These instances of such personnel accessing data without business need were independently detected by [Coinbase's] security monitoring in the previous months." Coinbase "immediately terminated the personnel involved and also implemented heightened fraud-monitoring protections and warned customers whose information was potentially accessed in order to prevent misuse of any compromised information."[6]

5. Though Coinbase continues to claim that "security and transparency are core to Coinbase," it provides a paltry amount of information concerning the Data Breach on its website, and does not position impacted individuals to protect themselves against fraud and identity theft. Indeed, it is clear that Coinbase customers (and perhaps others) have already experienced the fallout of the Data Breach. Coinbase acknowledged that "cybercriminals bribed and recruited a group of rogue overseas support agents to steal Coinbase customer data to facilitate social engineering attacks . . . . [and] to gather a customer list they could contact while pretending to be Coinbase—tricking people into handing over their crypto. They then tried to extort Coinbase for $20 million to cover this up."[7]

---

[4] *See* Coinbase Global, Inc., Form 8-K (May 14, 2025), https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm#:~:text=On%20May%2011%2C%202025%2C%20Coinbase%2C%20Inc..

[5] *See* Coinbase Global, Inc., Form 8-K (May 14, 2025), https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm#:~:text=On%20May%2011%2C%202025%2C%20Coinbase%2C%20Inc..

[6] *See* https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists (last accessed May 15, 2025).

[7] *Id.*

6. Coinbase stated that it is "continuing to review and bolster its anti-fraud protections to mitigate the risk that the compromised information could be used in social-engineering attempts. To the extent any eligible retail customers previously sent funds to the threat actor as a direct result" of the Data Breach, Coinbase "intends to voluntarily reimburse them after it completes its review to confirm the facts."[8]

7. While the financial impact is still being assessed and Coinbase hasn't revealed how many customers were deceived into sending funds to the cybercriminals in follow-up social engineering attacks, the company estimates that the resulting expenses will be "within the range of approximately $180 million to $400 million" for remediation and customer reimbursements.

8. Coinbase's failures to ensure that its servers and systems were adequately secure fell far short of its obligations and Plaintiff's and Class members' reasonable expectations for data privacy jeopardized the security of Plaintiff's and Class member's Personal Information, and exposed Plaintiff and Class members to fraud and identity theft or the serious risk of fraud and identity theft.

9. As a result of Defendants' conduct and the resulting Data Breach, Plaintiff's and Class members' privacy has been invaded, their Personal Information is now in the hands of criminals, they have either suffered fraud or identity theft or face an imminent and ongoing risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

10. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants inadequate safeguarding of Class Members' Personal Information that it collected and maintained.'

PARTIES

19. Plaintiff Allen Shakib is an adult citizen of the state of California and resides in Sherman Oaks, California. Plaintiff is a victim of the Data Breach. Defendants received Plaintiff's PII in connection with the services he received as a Coinbase customer. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

[8] *See id.*

Plaintiff has a continuing interest in ensuring that his Personal Information, which, upon information and belief, remains backed up in Coinbase's possession, is protected and safeguarded from future breaches.

20. Defendant Coinbase Global, Inc. is a Delaware corporation with its principal place of business located in One Madison Avenue Suite 2400 New York, New York 10010.

21. Defendant Coinbase, Inc. is a wholly owned subsidiary of Coinbase Global, Inc. and operates the Coinbase platform.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there are in excess of 100 Class members, the action is a class action in which one or more Class members are citizens of states different from Defendants.

23. The Court has personal jurisdiction over Coinbase. Until 2020, Coinbase maintained its headquarters in San Francisco, California. Upon information and belief, Coinbase routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State, has intentionally availed itself of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State. In addition, Plaintiff's claims arise out of or relate to Coinbase's business activities in California.

24. Venue properly lies in this judicial district because, *inter alia,* Coinbase transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Coinbase Collects and Stores Personal Information

25. Coinbase is the largest U.S. based cryptocurrency exchange, with over 100 million users and a trading volume of $468 billion.[9] Its stated purpose is to "increase economic freedom in the world"

[9] *See* Coinbase Global, Inc., Form 10-K (Feb. 13, 2025), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001679788/000167978825000022/coin-20241231.htm.

by "updat[ing] the century-old financial system by providing a trusted platform" to trade cryptocurrencies.[10]

26. Coinbase routinely collects highly sensitive Personal Information in the process of providing its services and claims to be the "most trusted place for people and businesses to buy, sell, and use crypto."[11]

27. Coinbase is and was aware of the sensitive nature of the Personal Information it collects, and it acknowledges the importance of data privacy.

28. Coinbase was aware of the need to safeguard the sensitive Personal Information entrusted to it by consumers as a necessary part of its business operations, stating as follows in a recent filing with the SEC:

> **Privacy and protection of user data**
>
> We are subject to a number of laws, rules, directives, and regulations relating to the collection, use, retention, security, processing, and transfer of personally identifiable information about our customers and employees in the countries where we operate. Our business relies on the processing of personal data in many jurisdictions and the movement of data across national borders. As a result, much of the personal data that we process, which may include certain financial information associated with individuals, is regulated by multiple privacy and data protection laws and, in some cases, the privacy and data protection laws of multiple jurisdictions. In many cases, these laws apply not only to third-party transactions, but also to transfers of information between or among us, our subsidiaries, and other parties with which we have commercial relationships.[12]

B. The Data Breach

29. On May 15, 2025, Coinbase publicly disclosed a Data Breach involving cybercriminals who recruited and bribed rogue overseas support agents to steal sensitive personal data from Coinbase's internal systems and then demanded a $20 million ransom not to publish the stolen information. Coinbase

[10] Investor Relations, COINBASE, https://investor.coinbase.com/home/default.aspx (last accessed May 15, 2025).

[11] https://www.coinbase.com

[12] *See* Coinbase Global, Inc., Form 10-K, https://www.sec.gov/ix?doc=/Archives/edgar/data/0001679788/000167978825000022/coin-20241231.htm (last accessed May 15, 2025).

has not paid the demand and is cooperating with law enforcement in the investigation of the Data Breach.[13]

30. According to Coinbase, on May 11, 2025, it "received an email communication from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase documentation, including materials relating to customer-service and account-management systems."[14] The cybercriminals "obtained this information by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems to which they had access in order to perform their job responsibilities. These instances of such personnel accessing data without business need were independently detected by [Coinbase's] security monitoring in the previous months." Coinbase "immediately terminated the personnel involved and also implemented heightened fraud-monitoring protections and warned customers whose information was potentially accessed in order to prevent misuse of any compromised information."[15]

31. Though Coinbase continues to claim that "security and transparency are core to Coinbase," it provides a paltry amount of information concerning the Data Breach on its website and does not position impacted individuals to protect themselves against fraud and identity theft. Indeed, it is clear that Coinbase customers (and perhaps others) have already experienced the fallout of the Data Breach. Coinbase acknowledged that "cybercriminals bribed and recruited a group of rogue overseas support agents to steal Coinbase customer data to facilitate social engineering attacks . . . . [and] to gather a customer list they could contact while pretending to be Coinbase—tricking people into handing over their crypto. They then tried to extort Coinbase for $20 million to cover this up."[16]

---

[13] *See* Coinbase Global, Inc., Form 8-K (May 14, 2025), https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm#:~:text=On%20May%2011%2C%202025%2C%20Coinbase%2C%20Inc. (last accessed May 15, 2025).

[14] *See* Coinbase Global, Inc., Form 8-K (May 14, 2025), https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm#:~:text=On%20May%2011%2C%202025%2C%20Coinbase%2C%20Inc. (last accessed May 15, 2025).

[15] *See* https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists (last accessed May 15, 2025).

[16] *Id.*

32. Coinbase stated that it "is continuing to review and bolster its anti-fraud protections to mitigate the risk that the compromised information could be used in social-engineering attempts. To the extent any eligible retail customers previously sent funds to the threat actor as a direct result" of the Data Breach, Coinbase "intends to voluntarily reimburse them after it completes its review to confirm the facts."[17]

C. Impact of the Data Breach

33. As a result of the Data Breach, Plaintiff and Class members had their most sensitive Personal Information "accessed" and "acquired" by cybercriminals, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, and unauthorized use of their Personal Information.

34. The actual extent and scope, and the impact, of the Data Breach on Coinbase's customers (or other affiliated persons) remains uncertain. Unfortunately for Plaintiff and Class members, the damage is already done because their sensitive Personal Information is confirmed by Coinbase to have been disclosed to unauthorized persons during the Data Breach.

35. Coinbase knew or should have known that its affected IT systems and/or servers are unsecure and do not meet industry standards for protecting highly sensitive customer Personal Information. On information and belief, Coinbase failed to timely make changes to its data security systems, privacy policies, and its IT systems and servers, exposing its customers' Personal Information to the risk of theft, identity theft, and fraud.

36. The Data Breach creates a heightened security concern for Plaintiff and Class members because their SSNs, financial information, and other sensitive information was potentially disclosed. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of his SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

[17] *See id.*

37. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[18] TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[19]

38. Coinbase had a duty to keep Plaintiff's and Class members' Personal Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class members provided their Personal Information to Coinbase with the understanding that Coinbase would comply with its Privacy Policy and its obligations to keep such information confidential and secure from unauthorized disclosures.

39. Defendants' data security obligations were particularly important given the substantial increase in data breaches in recent years, which are widely known to the public and to anyone in Coinbase's industry of financial services and crypto currency exchange operators.

D. Theft of Personal Information Has Serious Consequences for Victims

40. Data breaches are by no means new and they should not be unexpected. Business Insider has noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[20] It is well known amongst companies that store sensitive personally identifying information that sensitive Personal Information—like SSNs, financial information, tax information, etc.—is valuable and frequently targeted by criminals.

---

[18] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

[19] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[20] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last accessed March 16, 2025).

41. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, like Coinbase, and these companies must ensure that data privacy and security practices and protocols are adequate to protect against and prevent known and expected attacks.

42. Theft of Personal Information is serious. The Federal Trade Commission has warned consumers that identity thieves use Personal Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[21]

43. Indeed, with access to an individual's Personal Information, criminals can do more than simply empty a victim's bank account. They can also commit all manner of fraud, including: obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; obtain lending or lines of credit; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[22]

44. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[23]

---

[21] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed March 16, 2025).

[22] *See* FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed March 16, 2025).

[23] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed March 16, 2025).

45. Personal Information is a valuable property right.[24] The value of sensitive personal information as a commodity is measurable.[25] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[26]

46. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs, financial information, driver's license numbers, and other Personal Information directly on various illegal websites making the information publicly available, often for a price. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

47. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

48. Consumers place a high value on the privacy of sensitive data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[27]

---

[24] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[25] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[26] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[27] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

49. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[28]

50. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

51. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[29]

52. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Coinbase Failed to Act in the Face of a Known Risk of a Data Breach

53. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Defendants failed to take reasonable steps to adequately protect Personal Information, leaving its clients (and potentially others) exposed to risk of fraud and identity theft.

54. Coinbase is, and at all relevant times has been, aware that the sensitive Personal Information it handles and stores in connection with providing software services and products is highly sensitive. As a company that requires consumers to provide highly sensitive and identifying information, Coinbase is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

---

[28] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[29] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

55. Coinbase was aware, or should have been aware, of regulatory and industry guidance regarding data security, and was alerted to the risk associated with failing to ensure that Personal Information was adequately secured.

56. Despite the well-known risks of hackers and cybersecurity intrusions, Defendants failed to employ adequate data security measures in a meaningful way in order to prevent breaches, including the Data Breach.

57. The security flaws inherent to Defendants' IT systems or servers run afoul of industry best practices and standards. Had Defendants adequately protected and secured its servers or systems, and the sensitive Personal Information stored therein, it could have prevented the Data Breach.

58. Defendants permitted Class members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

59. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[30]

60. As a result of the events detailed herein, Plaintiff and Class members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

61. Victims of the Data Breach have likely already experienced harms and are subject to an imminent and ongoing risk of harm, including identity theft and fraud.

[30] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 30, 2017), https://www.reuters.com/article/idUSKBN18M2BY/.

62. As a result of Coinbase's failure to ensure that its impacted systems and servers were protected and secured, the Data Breach occurred. As a result of the Data Breach, Plaintiff's and Class members' privacy has been invaded, their Personal Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

CLASS ALLEGATIONS

63. Plaintiff brings this action on behalf of himself and the following Class pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**
> All residents of the United States who were impacted by the Data Breach, including all persons who were sent notice by Coinbase that their Personal Information was compromised as a result of the Data Breach.

64. Excluded from the Class are: (1) any Judge presiding over this action, members of their immediate families, and Court Staff; and (2) Defendants, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants, or its parents, have a controlling interest, and its current or former officers and directors.

65. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable. Upon information and belief, the proposed Class appear to include tens of thousands of members who are geographically dispersed.

66. **Typicality**: Plaintiff's claims are typical of Class members' claims. Plaintiff and all Class members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the Class members they seek to represent. Accordingly, Plaintiff's claims are typical of Class members' claims.

67. **Adequacy**: Plaintiff's interests are aligned with the Class Plaintiff seeks to represent, and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and undersigned counsel intend to prosecute this action vigorously. The Class' interests are well-represented by Plaintiff and undersigned counsel.

68. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class member's claims. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class members individually to effectively redress Defendants' wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

69. **Commonality and Predominance:** The following questions common to all Class members predominate over any potential questions affecting individual Class members:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants' data security practices resulted in the disclosure of Plaintiff's and other Class members' Personal Information and the Data Breach;
- whether Defendants violated privacy rights and invaded Plaintiff's and Class members' privacy; and
- whether Plaintiff and Class members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

70. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

71. **Injunctive and Declaratory Relief:** Consistent with Fed. R. Civ. P. 23(b)(2), Defendants, through its conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

72. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

73. Defendants was entrusted with, stored, and otherwise had access to the Personal Information of Plaintiff and Class members.

74. Defendants knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiff and Class members, and to not ensuring that its servers and systems, and the Personal Information, was secure. These risks were reasonably foreseeable to Defendants, including because Defendants have previously experienced a data breach.

75. Defendants owed duties of care to Plaintiff and Class members whose Personal Information had been entrusted to it.

76. Defendants breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate data security. Defendants had a duty to safeguard Plaintiff's and Class members' Personal Information and to ensure that their adequately protected Personal Information. Defendants breached this duty.

77. Coinbase's duty of care arises from its knowledge that its customers entrust it with highly sensitive Personal Information that Coinbase is required to, and represents that it will, handle securely. Indeed, on its website, Coinbase commits to data privacy in its Privacy Policy, including safeguarding sensitive Personal Information.

78. Only Coinbase was in a position to ensure that its systems, servers, and services were sufficient to protect against breaches and the harms that Plaintiff and Class members have now suffered.

79. A "special relationship" exists between Defendants, on the one hand, and Plaintiff and Class members, on the other hand. Defendants entered into a "special relationship" with Plaintiff and Class members by agreeing to accept, store, and have access to sensitive Personal Information provided by Plaintiff and Class members in connection with utilizing Coinbase's products and/or services.

80. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

81. Defendants acted with wanton disregard for the security of Plaintiff's and Class members' Personal Information.

82. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendants' breach of duties. Defendants knew or should have known they were failing to meet these duties, and that Defendants' breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Personal Information.

83. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class members have been harmed and face an imminent and ongoing risk of harm.

84. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

85. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

86. Coinbase provided or provides a platform for the exchange of cryptocurrency, and Plaintiff and Class members provided their Personal Information to Coinbase as users/customers or in otherwise transacting with Defendants.

87. In connection with their business relationship, Plaintiff and Class members entered into implied contracts with Coinbase.

88. Pursuant to these implied contracts, Plaintiff and Class members provided Coinbase with their Personal Information. In exchange, Coinbase agreed, among other things: (1) to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' Personal Information; and (2) to protect Plaintiff's and Class members' Personal Information in compliance with federal and state laws and regulations and industry standards.

89. The protection of Personal Information was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Coinbase, on the other hand. Had Plaintiff and Class members known that Coinbase would not adequately protect its customers' Personal Information they would not have done business with Coinbase.

90. Plaintiff and Class members performed their obligations under the implied contract when they provided Coinbase with their Personal Information.

91. Necessarily implicit in the agreements between Plaintiff/Class members and Defendants was Coinbase's obligation to take reasonable steps to secure and safeguard Plaintiff's and Class members' Personal Information.

92. Defendants breached its obligations under its implied contracts with Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect their Personal Information.

93. Defendants' breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach.

94. The damages sustained by Plaintiff and Class members as described above were the direct and proximate result of Defendants' material breaches of its agreements.

95. Plaintiff and other Class members were damaged by Defendants' breach of implied contracts because: (i) they have suffered actual harm or identity theft; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Personal Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Personal Information has been breached; (v) they were deprived of the value of their Personal Information, for which there is a well-established national and international market; (vi) they were deprived of the benefit of their bargain; and/or (vii) they lost time and money incurred to mitigate and remediate the effects of the breach, including the increased risks of identity theft they face and will continue to face.

COUNT VIII
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

96. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

97. This claim is pleaded in the alternative to the implied contract claim.

98. Coinbase has profited and benefited from the monies or fees paid and the Personal Information provided by Plaintiff and Class members to receive services from Coinbase.

99. Coinbase has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiff and Class members did not receive services of the quality, nature, fitness, or value represented by Coinbase and that reasonable consumers expected.

100. Coinbase has been unjustly enriched by its withholding of and retention of these benefits, at the expense of Plaintiff and Class members.

101. Equity and justice militate against permitting Coinbase to retain these profits and benefits.

102. Plaintiff and Class members suffered injury as a direct and proximate result of Coinbase's unjust enrichment and seek an order directing Coinbase to disgorge these benefits and pay restitution to Plaintiff and Class members.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and Class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiff and Class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and Class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Respectfully Submitted,

Dated: May 15, 2025

By: */s/ Tina Wolfson*

Tina Wolfson (SBN 174806)
Robert Ahdoot (SBN 172098)
Theodore W. Maya (SBN 223242)
Bradley K. King (SBN 274399)
AHDOOT & WOLFSON, PC
2600 West Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com
rahdoot@ahdootwolfson.com
tmaya@ahdootwolfson.com
bking@ahdootwolfson.com

Gary M. Klinger (pro hac vice to be filed)
MILBER COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Counsel for Plaintiff and the Proposed Class